# Отчёт по лабораторной работе 5

**Расширенная настройка HTTP-сервера Apache**

Авдадаев Джамал Геланиевич

# Содержание

# Список иллюстраций

# Список таблиц

# 1 Введение

## 1.1 Цель работы

Целью данной работы является приобретение практических навыков установки Rocky Linux на виртуальную машину с помощью инструмента Vagrant.

# 2 Процесс работы

## 2.1 Конфигурирование HTTP-сервера для работы через протокол HTTPS

В каталоге `/etc/pki/tls/private` был создан приватный ключ и самоподписанный сертификат для домена **www.dgavdadaev.net**. Использовалась команда генерации сертификата, после чего были введены параметры: RU, Russia, Moscow, dgavdadaev, dgavdadaev, dgavdadaev.net, dgavdadaev@dgavdadaev.net.

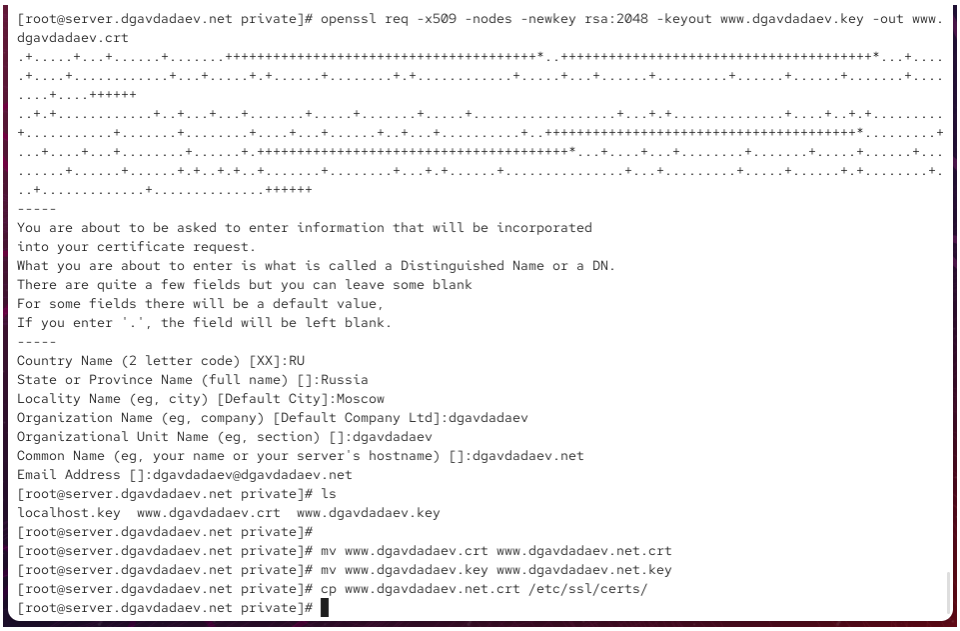


Рис. 2.1: Генерация ключа и сертификата

Сертификат и ключ были переименованы и размещены в соответствующих каталогах. Далее сертификат был скопирован в `/etc/ssl/certs/`.

Был отредактирован файл `/etc/httpd/conf.d/www.dgavdadaev.net.conf`, после чего он получил следующий вид:

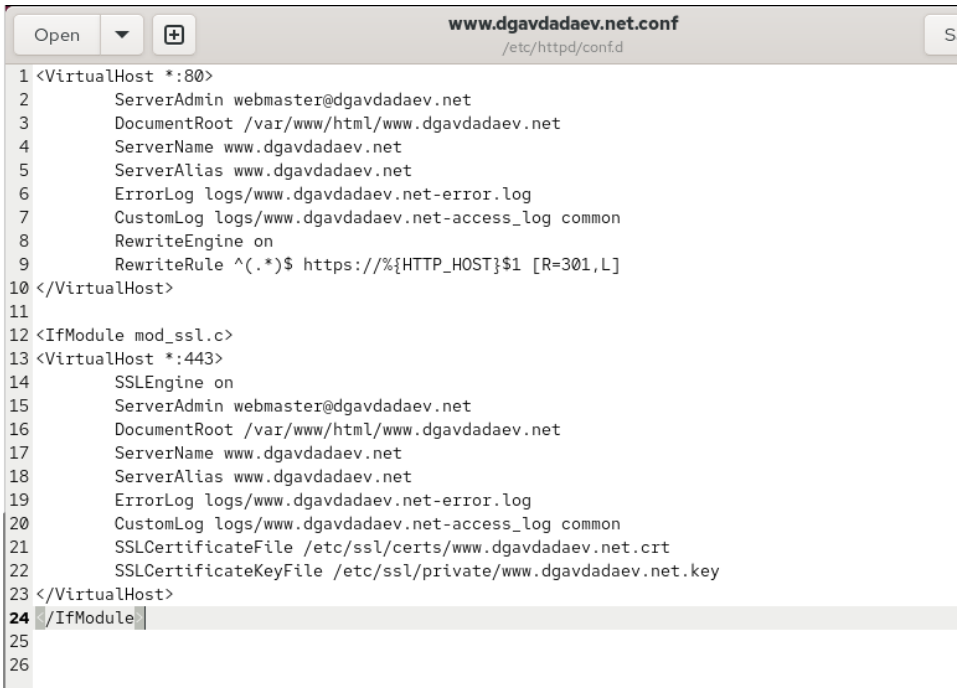


Рис. 2.2: Конфигурация Apache

### 2.1.1 Построчное пояснение конфигурации

- `<VirtualHost *:80>` — начало конфигурации виртуального хоста для HTTP.

- `ServerAdmin webmaster@dgavdadaev.net` — адрес администратора.

- `DocumentRoot /var/www/html/www.dgavdadaev.net` — корневая директория сайта.

- `ServerName` и `ServerAlias` — доменное имя сайта.

- `ErrorLog` и `CustomLog` — файлы логирования ошибок и обращений.

- `RewriteEngine on` — включение механизма переписывания ссылок.

- `RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]` — принудительное перенаправление всех запросов на HTTPS.

- `</VirtualHost>` — завершение блока HTTP.

- `<IfModule mod_ssl.c>` — проверка наличия модуля SSL.

- `<VirtualHost *:443>` — начало конфигурации HTTPS.

- `SSLEngine on` — включение SSL.

- Повторяются параметры администратора, домена, корневого каталога и логов.

- `SSLCertificateFile` — путь к сертификату.

- `SSLCertificateKeyFile` — путь к приватному ключу.

- `</VirtualHost>` — конец конфигурации HTTPS.

- `</IfModule>` — завершение условного блока.

После перезапуска веб-сервера сайт стал доступен по защищённому протоколу HTTPS.

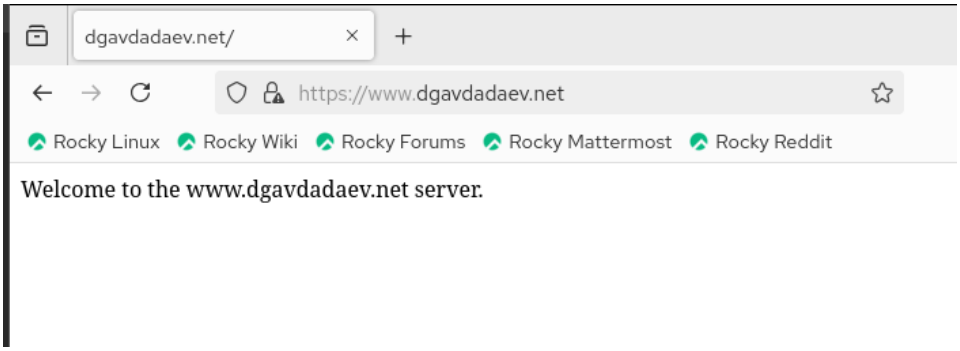


Рис. 2.3: Работа сайта по HTTPS

Просмотр сведений о сертификате показал корректность введённых параметров.

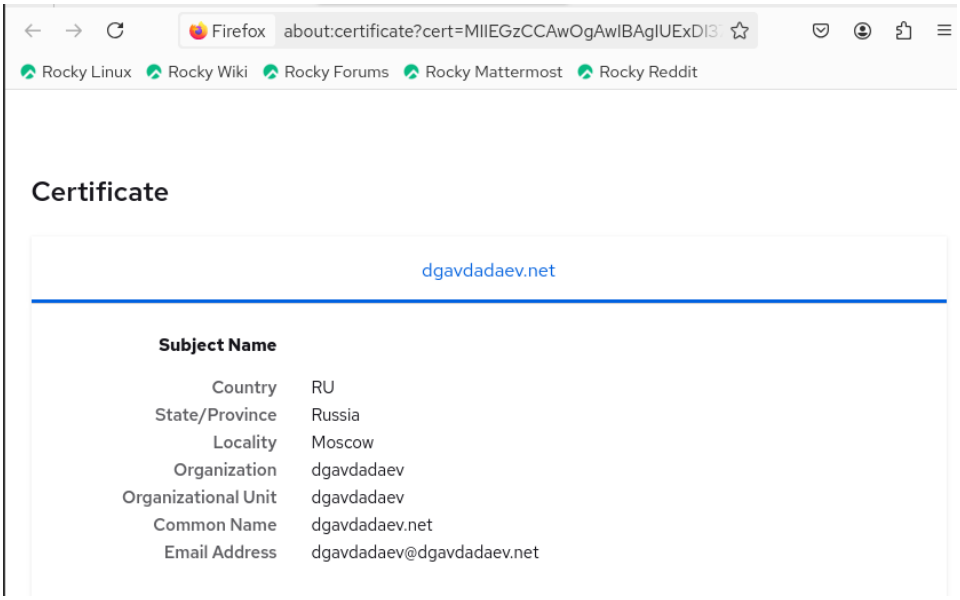


Рис. 2.4: Просмотр сертификата

## 2.2 Конфигурирование HTTP-сервера для работы с PHP

В каталоге сайта был создан файл `index.php` с функцией `phpinfo()`.

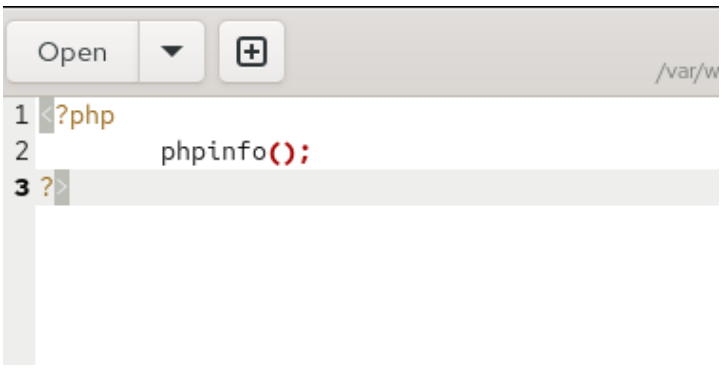


Рис. 2.5: Файл index.php

После выполнения всех настроек веб-сервер корректно обработал PHP-страницу.

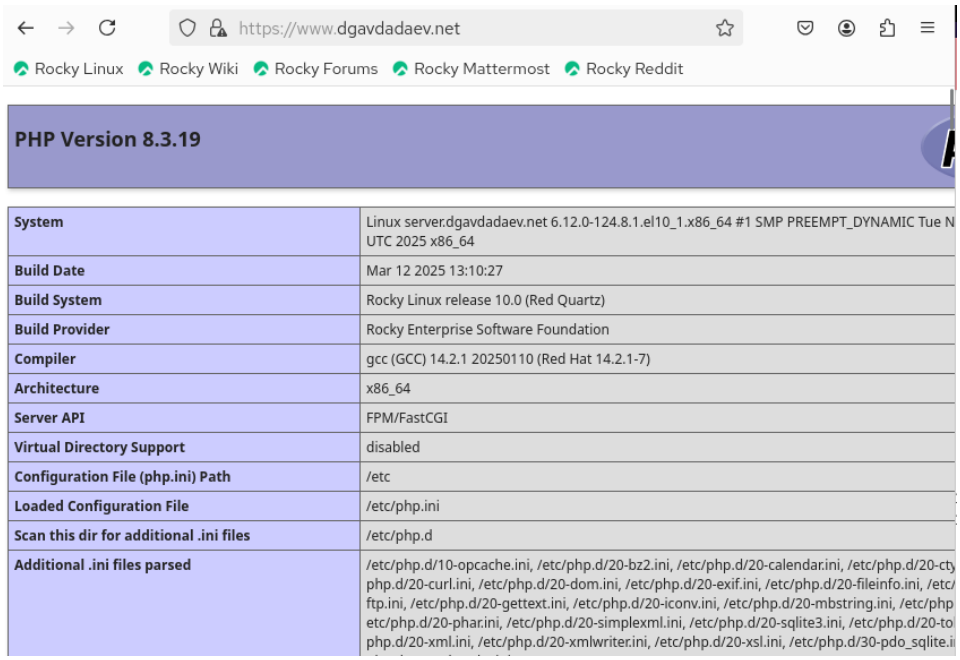


Рис. 2.6: Отображение phpinfo

## 2.3 Внесение изменений во внутреннее окружение виртуальной машины

В каталоге `/vagrant/provision/server/http` были размещены актуальные конфигурации веб-сервера. Для этого скопированы файлы Apache, веб-контента и SSL-материалов:

- конфигурации `/etc/httpd/conf.d/*` перенесены в `.../etc/httpd/conf.d/`;
- содержимое веб-каталога `/var/www/html/*` — в `.../var/www/html/`;
- созданы каталоги для ключей и сертификатов `etc/pki/tls/private` и `etc/pki/tls/certs`;
- файл приватного ключа и файл сертификата перенесены в соответствующие пути внутри `provision`.

```
[root@server.dgavdadaev.net www.dgavdadaev.net]# cp -R /etc/httpd/conf.d/* /vagrant/provision/server/http/etc/httpd/
conf.d/
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/autoindex.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/fcgid.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/manual.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/README'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/server.dgavdadaev.net.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/ssl.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/userdir.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/welcome.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/www.dgavdadaev.net.conf'? y
[root@server.dgavdadaev.net www.dgavdadaev.net]# cp -R /var/www/html/* /vagrant/provision/server/http/var/www/html/
cp: overwrite '/vagrant/provision/server/http/var/www/html/server.dgavdadaev.net/index.html'? y
[root@server.dgavdadaev.net www.dgavdadaev.net]#
[root@server.dgavdadaev.net www.dgavdadaev.net]# mkdir -p /vagrant/provision/server/http/etc/pki/tls/private
[root@server.dgavdadaev.net www.dgavdadaev.net]# cp -R /etc/pki/tls/private/www.dgavdadaev.net.key /vagrant/provisio
n/server/http/etc/pki/tls/private
[root@server.dgavdadaev.net www.dgavdadaev.net]# mkdir -p /vagrant/provision/server/http/etc/pki/tls/certs
[root@server.dgavdadaev.net www.dgavdadaev.net]# cp -R /etc/pki/tls/private/www.dgavdadaev.net.crt /vagrant/provisio
n/server/http/etc/pki/tls/certs/
[root@server.dgavdadaev.net www.dgavdadaev.net]#
```

Рис. 2.7: Копирование конфигурационных файлов

В скрипт `/vagrant/provision/server/http.sh` добавлены команды для установки PHP и правил межсетевого экрана, позволяющих работать через HTTPS. Это обеспечивает автоматическую подготовку окружения при развёртывании.

```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y groupinstall "Basic Web Server"
dnf -y install php

echo "Copy configuration files"
cp -R /vagrant/provision/server/http/etc/httpd/* /etc/httpd
cp -R /vagrant/provision/server/http/var/www/* /var/www
chown -R apache:apache /var/www
restorecon -vR /etc
restorecon -vR /var/www
echo "Configure firewall"
firewall-cmd --add-service=http
firewall-cmd --add-service=http --permanent
firewall-cmd --add-service=https
firewall-cmd --add-service=https --permanent
echo "Start http service"
systemctl enable httpd
systemctl start httpd

```

Рис. 2.8: Изменения в скрипте http.sh

# 3 Итоги

## 3.1 Вывод

В процессе работы был настроен веб-сервер для функционирования через HTTPS, создан самоподписанный сертификат, выполнено перенаправление с HTTP на HTTPS и добавлена поддержка PHP. Конфигурации и SSL-материалы перенесены во внутреннее окружение виртуальной машины для автоматического развёртывания. Проверена работа сертификата и корректное выполнение PHP-скриптов.

## 3.2 Контрольные вопросы

**1. В чём отличие HTTP от HTTPS?**

HTTP передаёт данные в открытом виде, тогда как HTTPS использует шифрование (TLS/SSL), обеспечивая защищённый канал между сервером и клиентом.

**2. Каким образом обеспечивается безопасность контента веб-сервера при работе через HTTPS?**

Безопасность достигается за счёт шифрования трафика, проверки подлинности сервера с помощью сертификата и защиты данных от перехвата и изменения.

**3. Что такое сертификационный центр? Приведите пример.**

Сертификационный центр (CA) — организация, выпускающая и подписывающая цифровые сертификаты, подтверждая подлинность владельца.
Примеры: LetsEncrypt, DigiCert, GlobalSign.